



THE DARK ECONOMY

Just how much do we stand to lose from internet threats such as spam and spyware? Simon Edwards sheds some light on cybercrime – and the real risks we face online

Internet threats such as computer viruses and hackers are deeply concerning. According to a report by anti-virus company Grisoft, 87 per cent of British citizens are worried about having their money stolen online. Grisoft found that people were more worried about cybertheft than burglary, assault or robbery. But how realistic are these fears?

It's tempting to think that viruses are written by spotty teenagers, that hackers are a Hollywood fantasy, and that spam is a threat only to those idiots who can't tell the difference between real email and fraudulent adverts for Viagra and pornography. However, as we will see, these stereotypes are completely outdated. Organised criminals are now using the internet and the latest hacking techniques to defraud regular users on a systematic basis. A new underground economy has evolved where our personal details are traded for cash on the internet. Criminal organisations provide services to others in a perverse mirror image of legitimate business. They even sell hacking tools in a web-based arms market.

Sometimes gangs engage in cyberwarfare, squabbling over territory. Instead of fighting over street corners and smuggling routes, they struggle to control large groups of home users' computers. These include the PCs and Macs that we use on a daily basis. Security firm Symantec

claims that 90 per cent of targeted attacks on the internet are aimed at home users.

SPAM TACTICS

Before we explore the underbelly of cybercrime, we need to classify the main internet threats that most of us face on a daily basis. Some, such as spam, seem fairly innocuous. This is because many people still assume that spam is about sending dodgy adverts by email. In fact, spam refers to any unsolicited email. This type of email can be far more sinister than special deals on Viagra.

Increasingly, spam is being used to deliver bad software directly to victims' desktops, links to infected sites and invitations to participate in a scam. For example, 'pump-and-dump' schemes involve distributing tips that encourage victims to buy shares in a company. When the price rises the fraudsters sell, thereby making a profit. The stock price drops following the sale, a situation made worse by the fact that the fraudsters are no longer hyping it, and the victims are left holding shares worth far less than their initial investment.

Spamming techniques are also used to distribute emails that purport to come from banks and other financial institutions. If you click on the links embedded in these emails, you won't end up at your online bank's login

page, although you'll think you have. These so-called phishing emails direct victims to convincing but fake copies of websites. Anyone who then enters their username and password will be handing valuable information directly to the criminals.

DRIVE-BY DOWNLOADS

You don't always need to enter any information to fall foul of a website. A website infected with spyware can attempt to download bad programs on to your PC. This type of attack has evolved to the point where the attacker no longer has to trick victims into installing Trojans, such as fake video-playing software. The software is quietly and automatically installed on the victim's system, and the user is none the wiser.

Spam can be used to direct you to spyware-infected sites under the control of the bad guys, but increasingly attackers are upping their game and infecting legitimate websites. In March 2008, anti-virus company Trend Micro's website was infected with malicious code that redirected visitors to spyware-laden sites in China.

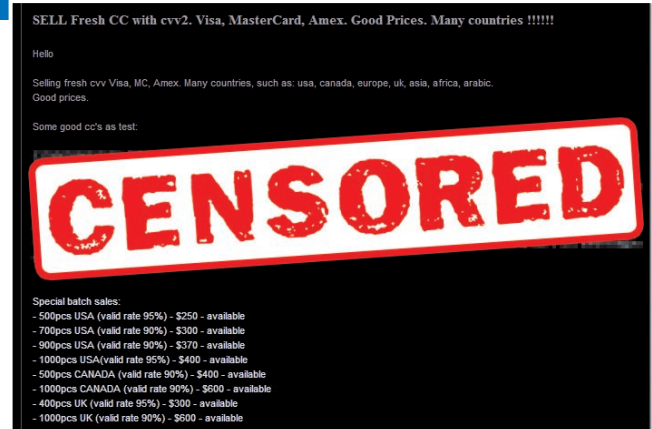
This technique of compromising trusted sites is becoming more and more popular with criminals. A month before Trend Micro's problem was noticed, an Indian security site was successfully infected. Last year, web-hosting company DreamHost was attacked and

Value judgements How much is your data worth?

According to internet infrastructure firm VeriSign, the average consumer is worth just over £10,000 online. This figure relates to the amount of money an individual holds in their online accounts. The company ran a survey that reported 43 per cent of people had experienced online identity fraud, or knew a victim of this type of crime. While surveys like this indicate how wealthy and concerned some internet users are, they don't investigate how much victims are worth from a criminal's point of view, nor do they take into account that each criminal will attribute a different value depending on their own criminal speciality. Such reports also fail to provide a useful illustration of the real risks that potential victims face.

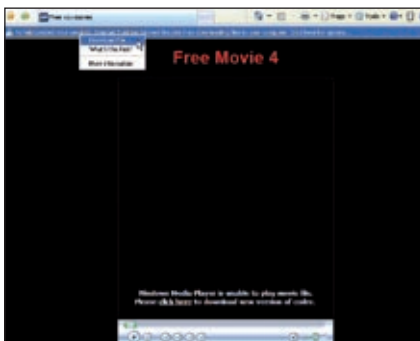
So how much is your data really worth? Symantec's latest report on internet security compiled a price list for credit card numbers, email passwords, bank account details and other valuable resources. These prices reflect what criminals are charging or paying when trading stolen information. Lists of credit card details were the most popular 'product', with an individual set of details costing between \$0.40 (around 20p) to \$20 (around £10). Bank accounts vary in price, depending on their balances. Symantec quotes a range between \$30 (around £15) to \$400 (around £200). According to Symantec, stolen information is most commonly sold in bulk, at a discount. The image above shows an advert for discounted batches of credit card details. We have covered the sample card numbers to protect the innocent.

This threat is reflected in the current card fraud figures. Over the past year, most credit card fraud in the UK involved transactions where



▲ This web-based forum shows criminals selling credit card numbers and other details; there are bulk discounts for batches of hundreds of records

the card was not physically present. This included internet transactions, as well as purchases made over the phone. According to APACS, the UK payments association, card fraud rose by 25 per cent in 2007, and fraud abroad now accounts for over a third of all losses. An estimated £290m was stolen in so-called card-not-present fraud – twice as much as counterfeit card fraud. Other frauds, such as those committed with lost or stolen cards, or card ID theft offences, were worth far less.



▲ A website that has been infected with spyware will often attempt to download bad programs to your computer without your knowledge

webpages belonging to its customers were infected. Even Google adverts have been used to attack victims, a situation that has been discussed in technical detail at <http://tinyurl.com/24nfq6>. The result is that you can no longer avoid spyware by visiting only trusted sites.

CONTROLLING INTEREST

Criminals tend not to launch spam and virus attacks from their own computers. Doing so would place them at increased risk of detection and arrest. It would also be relatively easy to block their attacks. Instead, they hijack other people's computers to do their dirty work.

Spyware and Trojans often connect the victim computer to large networks of similarly compromised systems. Each victim is known as a 'bot' and appears to work properly, so its owner is often none the wiser. However, they are all under the control of the attacker, who can issue commands to his 'botnet'. See the box on page 126 for details of how a botnet is spread.

Botnets can be used for a wide variety of nefarious purposes, including sending spam, viruses, links to virus-infected websites, phishing emails or denial-of-service (DoS) attacks. When a cybercriminal has control of hundreds of thousands of computers, he can send massive

amounts of data across the internet. The users of each individual computer probably won't even notice the small drain placed on the processor or network connection. Because of this, botnets are an important part of a cybercriminal's arsenal.

GETTING ORGANISED

Online threats have evolved to reflect their criminal nature. While early viruses were destructive, damaging files and causing obvious problems with the computer, modern ones are stealthier. This is because modern viruses have a job to do, whereas the older types were designed to satisfy the needs of vandals, egotists and the inappropriately curious. Researcher Sarah Gordon interviewed virus-writers in the mid-1990s and published a paper (<http://tinyurl.com/7vtcq>) that reported their motivations as including "relief from boredom, actively seeking fame, exploration, malice, and peer pressure".

This came to an end in 2004. In April of that year, anti-virus company Sophos reported that 69 per cent of all virus infections were variants of Netsky (www.sophos.com/security/top-10/200408.html). This virus was written by a German student called Sven Jaschan, who was arrested in May of the same year. Alex Shipp, senior anti-virus technologist and imagineer at security firm MessageLabs, recently told *Shopper* that Netsky was the "last of the spotty kid viruses". Following the release of this virus things changed, moving on to "organised crime, and the spam that comes as a result of that".

At least one version of the Netsky virus was designed to remove another virus if it found an infection on the same machine. It targeted Bagle, which was written by a different person or group. Security analysts at MessageLabs and other companies believe that Bagle was written by a criminal gang and that they were witnessing a battle between amateur and professional programmers. Alex Shipp notes that Netsky infections continued long after Bagle disappeared from the internet "so in a

way, the kid won". However, Bagle's authors have not been identified and are doubtless writing other viruses to this day.

CASH IN HAND

Today, most viruses, Trojans and other bad software are ultimately designed to make money. We've already looked at the ways in which online threats work, and some obvious ways in which they can steal valuable information. Once personal data is stolen, it can pass through many hands before becoming cold, hard cash. The underground economy, as we will see, is a sophisticated and complex system.

Trojans are a common threat. Regardless of how they are introduced to a victim's system, perhaps via spam or a drive-by download, they reside in the computer's memory and wait for the user to do something interesting. The Trojan might be activated when the user logs on to a banking or gambling website. The login details are then sent to the criminal, who then has a choice. He can use that information to extract money from the account, transferring it to one of his own, or he can pass the risk on to someone else by selling the details.

Stolen credit cards, bank account details and even online games accounts all have their price on the online black market. In its 2007 Internet Security Threat Report, Symantec reported that credit card numbers were selling for between \$0.40 (around 20p) and \$20 (around £10) each, with cards from the European Union considered more valuable than US cards. Stolen identities are also available, with European data costing more than American IDs. See the 'Value judgements' box above to see what specific personal details are worth.

Even online games accounts have a black market value. Symantec claims that "the total annual wealth created within virtual worlds has been placed at approximately \$10 billion". Currently, there are Trojans that target World of Warcraft players, as well as fans of games that are mainly popular in Asia, including Lineage. ➔



Symantec reports that in the first six months of 2007, five per cent of the top 50 malicious code samples reported to the company tried to steal account information for online games. "This is likely [because] there is considerable financial gain to be made from online gaming accounts, so attackers are deploying these threats in substantial numbers," it said.

Some malware is designed to recruit victim computers into vast armies of PCs under the control of the criminal. While this process doesn't steal money directly, it can be used to raise funds. Security companies have evidence that suggests the controllers rent out the use of their botnets, allowing them to send spam, spread other malware or attack specific computer systems. If you have control of a million home computers, you have a significant resource that can be used to overwhelm large, commercial sites. By requesting webpages, or simply sending small amounts of network traffic, all these computers working together can swamp the processing power and network bandwidth of a victim site.

SMOOTH OPERATORS

It's not hard to imagine amateur hackers selling credit card numbers to each other. However, beneath this near-to-surface threat is a better-hidden word of commerce, where organised criminals buy and sell victims' personal details, custom-made viruses, criminal internet services and knowledge of valuable and secret ways to break into computers.

Today's online criminals don't work alone. Not only do online criminal gangs exist, but they even specialise and provide illegal services to each other. Maksym Schipka, senior architect at MessageLabs, had this to say: "Most malware authors do not distribute it themselves. Instead, they offer their software 'for educational purposes'. Maybe they think that they can avoid prosecution."

A cybercriminal could buy an exploit and write software that uses the exploit to break into systems, but for many an easier and cheaper option is to commission someone else to write a bespoke Trojan or virus. Legitimate companies are starting to adopt a new business model commonly called Software as a Service (SaaS), where they sell software on a subscription basis, and online criminals are copying this way of working. Malware as a Service (MaaS) businesses are currently trading on the internet, selling access to bad software.

Targeted attacks, where viruses or Trojans are written to compromise a specific target, are available on the web at a range of prices. Andrew Lee, CTO of anti-virus company Eset, told *Shopper* that it is hard to gauge how common targeted attacks are "due to their nature". However, he notes that it is possible to buy customised malware that has been guaranteed to be undetectable by current anti-virus software for at least a short time. "They can be sold for anything between €600 (around £480) to €10,000 (around £8,000)," he said.

The availability of custom Trojans has doubtless made industrial espionage much easier. There is now a growing legitimate industry in preventing data leakage. While much of the danger comes from insiders leaking data, there is also a problem with malware being used to steal company information. This is because it is relatively easy to commission a

Is your computer safe? Identifying the threat in different systems

In most cases, technical threats have been designed to compromise Windows PCs, but we can expect other computer systems to grab the interest of online criminals. Windows PCs are not hacked because Windows is inherently less secure than other systems. Windows is popular with hackers because most potential victims use Windows. As Macintosh PCs become increasingly popular, security companies are reporting growth in Mac OS X spyware (see <http://tinyurl.com/5d955b> for more details).

Linux PCs are not invulnerable, either. Although they are attacked less often than Windows, security patches are frequently issued by different Linux distributions, and viruses, worms and Trojans all exist.

Currently, there are very few viruses for mobile phones. According to most security companies, this is due to the



wide variety of operating systems running on those phones. If manufacturers eventually settle on just one or two operating systems, and their customers use phones to hold valuable data, we can expect threats to appear in greater numbers. Anti-virus companies such as Symantec, Kaspersky and F-Secure provide security software for Symbian and Windows Mobile-based phones. Games consoles with internet access are vulnerable to attack and, as they are used to play online games, they could present an attractive target to criminals who want to steal games account information. The Xbox and Nintendo Wii both suffered from security breaches in 2007, demonstrating that not only are they potentially hackable but also that people are already viewing these devices as potential victims.

◀ A critical security flaw in the Xbox 360 was exploited by hackers last year

custom Trojan with which you can target the organisation of your choice.

Targeted attacks can be used for military purposes, too. According to the book *Crimeware: Understanding New Attacks and Defenses* (Symantec Press), written by Markus Jakobsson and Zulfikar Ramzan, several Trojans that used vulnerabilities in Microsoft Office came to light in 2006. The authors claim that the Trojans were linked to China, and that analysts have suggested the frequency and sophistication of the attacks indicate government sponsorship. Furthermore, they say that "whether this is a state-sponsored activity in these cases, all parties agree that custom malware (and especially Trojans) has been added to the military arsenal of many countries".

WHERE'S THE TRUST?

The criminal economy suffers from some of the troubles that plague everyday businesses. For example, it seems that virus-writers have a problem holding on to their intellectual property. While some authors will write new programs to fulfil the demand for custom Trojans, charging large amounts of money, there is plenty of evidence to suggest that online criminals steal programming code from each other, reselling the bad software for an easy profit.

Symantec notes that a malicious web browser exploit toolkit called MPack was pirated and sold at the "clearance sale" price of \$150 (around £75), which is a massive 85 per cent discount from the original \$1,000 (around £500) price. The company's weblog (<http://tinyurl.com/6jfoq6>) adds: "The sellers likely didn't even need to buy it themselves. [They] probably found some of the multiple websites that did not employ standard website protections, allowing them to download the whole kit for free."

As well as stolen goods, money can be swiped, too. When criminals cooperate, trust becomes an issue for them, particularly where

financial transactions with other criminals take place. Would you trust a faceless criminal who promises to provide an exploit, virus or other service to deliver after you've paid him? If you were the service provider, would you trust that your criminal client would pay once you'd fulfilled your side of the bargain?

Just as in the legal economy, there is a need for a trusted third party to proxy deals and ensure that funds are released reliably and only when the goods or services have been supplied. MessageLabs' Maksym Schipka explains: "A buyer will transfer payment to the guarantor and the seller will transmit the virus code or the credit card numbers. If the goods check out, the funds are released. Typically, these guarantors take two to three per cent of the transaction value for their services."

Money laundering is a well-established criminal practice and there are many ways to process funds, making it hard to trace their origin. Online criminals who deal with stolen personal and financial information need a way to turn this data into money fast so it can be laundered. Luckily for them, other criminals offer services that help.

Some middlemen specialise in selling personal data or convert stolen financial details, such as credit card numbers, into cash. One method is to use a 'drop service'. The middleman will pay a drop to receive goods bought with a stolen credit card number, or using other stolen financial details. The goods are sent on or sold immediately. The risk of being caught lies with the drop, not the cybercriminals. A drop can expect to earn between 10 and 50 per cent of the product's resale value.

NET WORTH

Some criminals specialise in controlling large botnets. These 'bot herders' charge for temporary use of parts of these networks. If you want to spread a Trojan or attack a website, it is usually cheaper and easier to pay someone to do



this for you, rather than develop the skills necessary to create your own botnet.

There are middlemen who buy malicious code and pay for the operator of a botnet to distribute it to victims. MessageLabs has compiled a sample price list for bot infection services, and claims that the charge for infecting 1,000 systems in the UK is \$60 (around £30). The same number of infections in Australia is worth \$100 (around £50), while the cost of infecting 1,000 Asian computers is just £3. These figures demonstrate that the geographical location of the victims makes a big difference in their value to criminals.

The sheer size of some botnets makes them a useful tool for blackmailers. Imagine a major sporting event, such as the Grand National, is about to take place. A blackmailer could rent a botnet and send a demand for £100,000 to an online bookmaker, threatening to remove its site in the run-up to the race. The amount of money the business would lose by being offline might be far greater than £100,000.

Online extortion, with the threat of a denial-of-service (DoS) attack if payment isn't received, does happen. Occasionally, a threat makes it into the news, as was the case with The Million Dollar Homepage in January 2006. When the owner, 21-year-old student Alex Tew, refused to pay a \$5,000 (around £2,500) ransom, his site was hit by a DoS attack. The criminals then demanded \$55,000 (around £27,500) to halt the attack. When he further refused, his site was hacked into and defaced.

THE HOLE TRUTH

Spyware programs and other software used for breaking into computers need to exploit a vulnerability in the victims' systems. This will usually be a security hole in the operating system or software such as the web browser. All personal computers can be hacked, whether they run Windows, Linux or even Mac OS X (see 'Is your computer safe?' on page 124). As security problems are found with these systems, fixes are issued by the vendors. This is why Microsoft makes frequent updates to Windows. It is also the reason why any recent Linux distribution has an automatic update utility and why Apple issues fixes for OS X.

Legitimate security researchers find security holes in products and notify the vendor, which creates a fix. The problem here is that it's not just the good guys who are looking for holes, and

there is a thriving black market in 'zero-day' exploits that can be used to hack into systems. As the vendor is unaware of the problem, it won't be able to fix it.

It's hard to judge the cost of a zero-day exploit on this most secretive part of the black market, but we can guess, because this type of information is also sold legally. Adriel Desautels, chief technology officer for security firm Netragard, claims to have brokered legal deals where information about new security flaws changed hands for more than \$75,000 (around £37,500). He reportedly told security website SecurityFocus that exploits have been sold for "as much as \$120,000 (£60,000)".

In its 2007 Criminology Report, security company McAfee said: "In January 2006, a Microsoft WMF exploit was sold in an online auction for \$40,000 (around £20,000), allegedly to more than one cybercriminal. Investigations revealed that the exploit was used by at least one buyer to capture machines to spread pump-and-dump spam, email campaigns designed to inflate stock prices with bogus insider information. This is just one example of a relatively low-priced exploit. Some can fetch up to \$75,000 (around £37,000)."

The trading of zero-day exploits amounts to a virtual arms trade. In itself, this is not an illegal situation in every country. However, even if it were, it would be hard to control. The actual use of these exploits could break a number of well-established laws, though. The 'weapons' bought and sold can be used to attack systems directly, which would break computer-misuse laws, or merely threaten an attack. Blackmail, which is also illegal, is one possible route a criminal could take when armed with an 'unknown' exploit that could break into a computer system.

LOOKING TO THE FUTURE

Most visible internet threats exist to make money, usually by stealing or scamming it from victims. While many criminals seem happy to target home users, there's nothing to say they won't accept payment from clients who want to participate in corporate espionage and even military and terrorist actions. There is evidence to suggest such attacks have already happened.



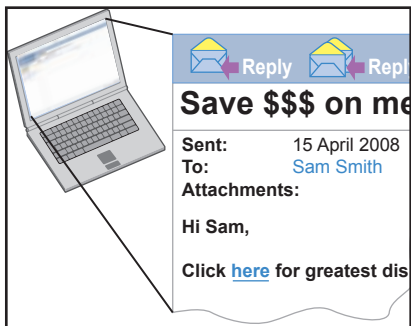
▲ The Million Dollar Homepage website suffered a distributed denial-of-service attack when the website's creator Alex Tew refused to pay the large ransom demanded by cybercriminals

The idea of terrorists hacking the US water system or power grid is the stuff of a Hollywood blockbuster, but online crime can easily serve terrorist agendas, and it would be naive to believe that terrorist groups were ignoring the rich source of money available online. Even if they don't use hacking techniques to attain their ultimate goals, terrorists could use cybercrime to fund more conventional terrorist missions.

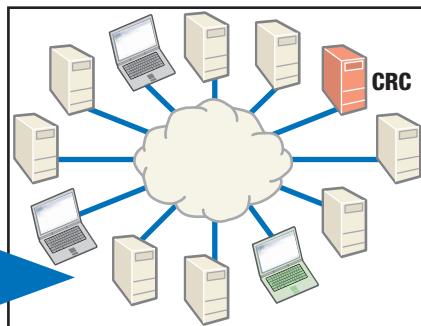
Using botnets to unleash a DoS attack is one way to inconvenience your political enemies, but it won't win any wars. However, there have been cases of political activists using internet attacks to make their point. When Estonia's financial and state servers were brought down in April 2007, Russia was suspected even though an Estonian, Dmitri Galushkevich, was arrested. China is suspected of being behind the 'Titan Rain' cyber attacks on the systems of Western governments. Suleyman Anil, head of Nato's computer incident response centre, claims such attacks do occur and predicts they will continue. He also believes such attacks are "practically impossible to stop".

In principle, there is no reason why dramatic attacks on power, air control and defence systems could not be made successfully in certain circumstances. Say a disenfranchised minority group wishes to damage what it considers to be a repressive government. It could be more economical, financially and in terms of manpower, to attack central services over the internet than to send in suicide bombers or plan a more sophisticated attack. **CS**

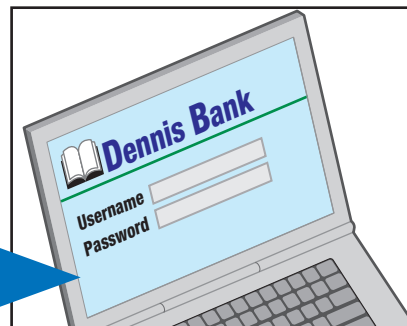
How the botnet spreads The life cycle of a botnet



▲ A victim receives a spam email containing a link to a website. Clicking on this loads a spyware-infected page that installs malicious software



▲ The victim's PC communicates with the criminal's command and control (C&C) system. This controls many other infected systems, which form a botnet



▲ The C&C system tells the bots to send spam and phishing mails to other potential victims. They may contain links to infected sites or fake bank sites